1. A system for securely storing medical data, comprising

an input process allowing an individual to enter identity information and medical data to associate with the identity information,

an encryption key process for providing to each individual an encryption key for encrypting medical data associated with the individual, and

a data table generator for storing medical data including encrypted medical data, in a table, whereby stored medical data from different individuals may be encrypted with different encryption keys.

2. A system according to claim 1, further comprising

a key table generator for storing the encryption key in a key table.

3. A system according to claim 1, wherein the input process includes

a private identity generator for generating for an individual a unique private identity being generated independently of the identity information.

4. A system according to claim 3, wherein the private identity generator includes a random number generator for generating a random number for the private identity.

5. A system according to claim 3, wherein the random number generator is selected from the group consisting of

6. A system according to claim 3, further including

means for employing the private identity as a relational link key for relating medical data associated with the individual to the encryption key associated with the individual.

7. A system according to claim 3, wherein the encryption key process includes

a process for generating the encryption key as a function of the private identity.

8. A system according to claim 3 wherein the encryption key process includes a process for generating the encryption key as an asymmetric function of the private identity.

9. A system according to claim 3 wherein the encryption key process includes a process for generating the encryption key as a symmetric function of the private identity.

10. A system according to claim 2, further including a table encryption process for encrypting the key table to secure the encryption key stored therein.

11. A system according to claim 3, further comprising a relational link generator for processing the private identity to generate a relational link for associating medical data in the data table with a respective private identity.

12. A system according to claim 11, wherein the relational link generator includes a process for processing the private identity selected from the group consisting of a symmetric key algorithm, an asymmetric key algorithm, an asymmetric key algorithm, and a hash algorithm.

13. A system for storing medical data, comprising an input process for allowing an individual to enter identity information and medical data to associate with the identity information, a private identity generator for generating independent of the identity information, a unique private identity for the individual,

an encryption key process for providing to the individual a respective encryption key for encrypting the medical data of the individual,

a relational link generator for providing relational links for the medical data and the encryption key associated with the individual, whereby the medical data and encryption key can be stored in a table of a relational database.

14. A system according to claim 13, wherein the relational link generator includes an encryption process for encrypting a relational link for accessing medical and/or the encryption key.

15. A system according to claim 13, wherein the relational link generator includes a hash process for generating a relational link as a hash function of the private identity.

16. A system according to claim 13, wherein the private identity generator includes a random number generator for generating the private identity as a function of a random number.

17. A system according to claim 16, wherein the relational link generator includes a process for encrypting the private identity to provide an encrypted relational link.

18. A process for controlling access to medical data, comprising:

allowing an individual to provide medical data and identity information,

providing the individual with a private identity and storing the medical data and identity information in tables of a relational database employing the private identity to provide a relational link to the medical and identity data,

employing the private identity to create an encryption key for the respective individual, and

encrypting, as a function of the encrypting key, medical data associated with the

individual, whereby medical data of different individuals are encrypted with different respective encryption keys.

19. A process according to claim 18, further comprising:
allowing a medical professional to search the relational database to identify medical data of interest.

20. A process according to claim 18, further comprising:
allowing a medical professional to request identity information associated with medical data in the relational data base, and employing the private identity to notify the respective individual of the request.

21. A process according to claim 18, further comprising:
allowing the individual to control access to the medical data of the individual.

22. A process according to claim 18, further comprising:
allowing the individual to store portions of the medical data in the clear and portions in an encrypted form.

23. A process according to claim 22, comprising:
allowing a medical professional to search the relational database.